Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims

Claim 1 (Currently amended): A communication system having a server for providing a Web E-mail service to a client, wherein said server comprises:

management means for managing a key for decrypting an encrypted E-mail;

authentication means for executing authentication of the use allowance of the managed key to said client when said client requests to decrypt the encrypted E-mail;

decrypting means for decrypting ~~said~~ the encrypted E-mail using ~~said~~ the managed key in the case where the use allowance is authenticated by said authentication means; and

transmission control means for controlling ~~said decrypted~~ to transmit the E-mail ~~thereby to transmit said decrypted E-mail~~ decrypted by said decrypting means to said client through a Web.

Claim 2 (Cancelled)

Claim 3 (Currently amended): The communication system according to claim ~~2~~ 1, wherein said authentication means provides said client with a window data to authenticate the use allowance of ~~said~~ the managed key.

Claim 4 (Currently amended): The communication system according to claim ~~2~~ 1, wherein said authentication means authenticates the use allowance using a passphrase inputted from said client.

Claim 5 (Currently amended): The communication system according to claim ~~2~~ 1, wherein said authentication means authenticates the use allowance ~~using~~ based on a biometrics

PAGE 3/16 * RCVD AT 6/29/2005 7:10:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-38

information of a user inputted from said client.

Claim 6 (Currently amended): The communication system according to claim 1, wherein said server further comprises encryption communication means for establishing and communicating a Web encryption communication when ~~communicating~~ starting to communicate with said client through the Web.

Claim 7 (Currently amended): The communication system according to claim ~~2~~ 1, wherein said server further comprises the encryption communication means for establishing and communicating ~~the~~ a Web encryption communication when ~~communicating~~ starting to communicate with said client through the Web~~, and transmission means for transmitting the use allowance by said~~ before the authentication executed by authentication means and the transmission of the decrypted E-mail ~~decrypted by said decrypting means to said client after the Web encryption communication is established by said encryption communication means~~ by said transmission control means.

Claim 8 (Currently amended): The communication system according to claim 7, wherein said authentication means authenticates the use allowance of ~~said~~ the managed key ~~in units of~~ during a session of ~~an~~ the Web encryption communication continuously established between said client and ~~a~~ server.

Claim 9 (Currently amended): The communication system according to claim 8, wherein said authentication means stops said authenticated use allowance, in the case where at least either the case where ~~said~~ the Web encryption communication is ended with an error or the case where ~~said~~ the Web encryption communication has passed a fixed time is satisfied.

Claim 10 (Currently amended): The communication system according to claim 1, wherein said server further comprises signature means for executing a digital signature to an E-mail ~~required~~

PAGE 4/16 * RCVD AT 6/29/2005 7:10:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-38

~~for the digital signature~~ created by said client.

Claim 11 (Currently amended): The communication system according to claim 1, wherein said server further comprises:

~~management~~ multiple use judging means for ~~managing~~ judging whether ~~said~~ the managed key is under multiple use, and

~~said management means comprises~~ stop means for stopping the use allowance of ~~said~~ a session under multiple use in the case where ~~said~~ the session is judged to be under multiple use by said multiple use judging means.

Claim 12 (Currently amended): The communication system according to claim 1, wherein the key for decrypting ~~said~~ the encrypted E-mail is a secret key in a code of a public key cryptosystem.

Claim 13 (Currently amended): ~~The~~ A communication system ~~comprising~~ having a client receiving a Web E-mail service from a server, wherein the server comprises:

management means for managing a key for decrypting an encrypted E-mail;

authentication means for executing authentication of the use allowance of the managed key to said client based on authentication information sent from said client when said client requests to decrypt the encrypted E-mail;

decrypting means for decrypting ~~said~~ the encrypted E-mail using ~~said~~ the managed key in the case where the use allowance is authenticated by said authentication means; and

transmission control means for controlling to transmit the E-mail decrypted by said decrypting means to said client through a Web,

and ~~a client receiving a Web E-mail service from a server including transmission control means for controlling said decrypted E-mail so as to transmit to said client through the~~

PAGE 5/16 * RCVD AT 6/29/2005 7:10:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-38

~~Web,~~

wherein said client comprises ~~the use allowance means for executing use allowance of the key for decrypting said encrypted E-mail to said server, and~~

request means for requesting to decrypt the encrypted E-mail;

authentication information sending means for sending the authentication information to said authentication means; and

receiving means for receiving the decrypted E-mail ~~decrypted by said server~~ transmitted by said transmission control means through the Web.

Claim 14 (Currently amended): A method for controlling a communication system including a server for providing ~~the~~ a client with ~~the~~ a Web E-mail service, comprising:

a management step of managing a key for decrypting an encrypted E-mail;

an authentication step of executing authentication of the use allowance of the managed key to said client when said client requests to decrypt the encrypted email;

a decrypting step of decrypting ~~said~~ the encrypted E-mail using ~~said~~ the managed key in the case where the use allowance is authenticated in said authentication step; and

a transmission control step of controlling ~~said decrypted~~ to transmit the E-mail decrypted in said decrypting step ~~to transmit~~ to said client, in the server.

Claim 15 (Cancelled)

Claim 16 (Currently amended): A method for controlling the communication system according to claim ~~15~~ 14, wherein, in said authentication step, a window data for authenticating the use allowance of ~~said~~ the managed key is supplied to said client for authentication.

Claim 17 (Currently amended): A method for controlling the communication system according to claim ~~15~~ 14, wherein, in said authentication step, the use allowance is

PAGE 6/16 * RCVD AT 6/29/2005 7:10:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-38

authenticated using a passphrase inputted from said client.

Claim 18 (Currently amended): A method for controlling the communication system according to claim ~~15~~ 14, wherein, in said authentication step, the use allowance is authenticated ~~using~~ based on biometrics information of a user inputted from said client.

Claim 19 (Currently amended): A method for controlling the communication system according to claim 14, wherein, in said server, the method further comprises an encryption communication step of establishing and communicating the Web encryption communication when ~~communicating~~ starting to communicate with said client through the Web.

Claim 20 (Currently amended): A method for controlling the communication system according to claim ~~15~~ 14, in said server, further comprising the encryption communication step of establishing and communicating ~~the~~ a Web encryption communication when ~~communicating~~ starting to communicate with said client through the Web~~, and a transmission control step of transmitting use allowance in said~~ before the authentication executed in the authentication step and the transmission of the decrypted E-mail ~~decrypted by said decrypting step to said client after the Web encryption communication is established in said encryption communication step~~ in said transmission control step.

Claim 21 (Currently amended): A method for controlling the communication system according to claim 20, wherein, in said authentication step, the use allowance of ~~said~~ the managed key is authenticated ~~in units of~~ during a session of ~~an~~ the Web encryption communication continuously established between said client and ~~a~~ server.

Claim 22 (Currently amended): A method for controlling the communication system according to claim 21, wherein, in said authentication step, said authenticated use allowance is stopped in the case when at least either the case where ~~said~~ the Web encryption communication

PAGE 7/16 * RCVD AT 6/29/2005 7:10:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-38

is ended with an error or the case where ~~said~~ the Web encryption communication has passed a fixed time is satisfied.

Claim 23 (Currently amended): A method for controlling the communication system according to claim 14, further comprising a signature step of executing the digital signature to the E-mail ~~required for the digital signature from~~ created by said client in said server.

Claim 24 (Currently amended): A method for controlling the communication system according to claim 14, further comprising a step of executing a ~~management~~ multiple use judging step of ~~managing~~ judging whether ~~said~~ the managed key is under multiple use in the server, ~~said management step including~~ and a stop step of stopping the use allowance of ~~the~~ a session under multiple use in the case where the session is judged to be under multiple use in said multiple use judging step.

Claim 25 (Currently amended): A method for controlling the communication system according to claim 14, wherein the key for decrypting ~~said~~ the encrypted E-mail is a secret key in an encryption of a public key cryptosystem.

Claim 26 (Currently amended): A method for controlling a communication system including a client receiving a Web E-mail service from a server, comprising a step of executing a management step of managing a key for decrypting an encrypted E-mail, an authentication step of executing authentication of the use allowance of the managed key to said client based on authentication information sent from said client when said client requests to decrypt the encrypted E-mail, a decrypting step of decrypting ~~said~~ the encrypted E-mail using ~~said~~ the managed key in the case where the use allowance is authenticated in said authentication step, and a transmission control step of controlling ~~said decrypted~~ to transmit the E-mail decrypted in said decrypting step ~~so as to transmit~~ to said client in the server, wherein said client comprises

PAGE 8/16 * RCVD AT 6/29/2005 7:10:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-38

~~comprising a step of executing a use allowance step of executing the use allowance of the key of decrypting said encrypted E-mail,~~ a requesting step of requesting to decrypt the encrypted E-mail, an authentication information sending step of sending the authentication information for authentication in said authentication step, and a receiving step of receiving the decrypted E-mail ~~decrypted by said server in~~ transmitted in said transmission step to the client.

Claim 27 (Currently amended): A computer executable control program of a communication system including a server for providing a Web E-mail service to a client, said program comprising a management step of managing a key for decrypting an encrypted E-mail, an authentication step of executing authentication of the use allowance of the managed key to said client when said client requests to decrypt the encrypted E-mail, a decrypting step of decrypting ~~said~~ the encrypted E-mail using ~~said~~ the managed key in the case where the use allowance is authenticated in said authentication step, and a transmission control step of controlling ~~said decrypted~~ to transmit the E-mail ~~so as to transmit~~ decrypted in said decrypting step to said client.

Claim 28 (Currently amended): A control program of a communication system including a client receiving a Web E-mail service through a Web from a server, comprising a step of executing a management step of managing a key for decrypting an encrypted E-mail, an authentication step of executing authentication of the use allowance of the managed key to said client based on authentication information sent from said client when said client requests to decrypt the encrypted E-mail, a decrypting step of decrypting ~~said~~ the encrypted E-mail using ~~said~~ the managed key in the case where the use allowance is authenticated in said authentication step, and a transmission step of controlling ~~said decrypted~~ to transmit the E-mail ~~so as to transmit~~ decrypted in said decrypting step to said client in the server, and said client

comprising a ~~step of executing a use allowance step of executing the use allowance of the key for decrypting said encrypted E-mail to said server~~ requesting step of requesting to decrypt the encrypted E-mail, an authentication information sending step of sending the authentication information for authentication in said authentication step, and a receiving step of receiving the decrypted E-mail ~~decrypted by said server in~~ transmitted in said transmission step to the client.

Claim 29 (Currently Amended): A storage medium storing a computer executable control program of a communication system including a server of providing a Web E-mail service to a client, the program comprising a step of executing a management step of managing a key for decrypting said encrypted E-mail using said managed key, an authentication step of executing authentication of the use allowance of the managed key to said client when said client requests to decrypt the encrypted E-mail, and a transmission control step of controlling ~~said decrypted~~ to transmit the decrypted E-mail ~~so as to transmit~~ to said client in a server.

Claim 30 (Original): A storage medium storing a control program of a communication system including a client receiving a Web E-mail service through a Web from a server, wherein the program comprises a step of executing a management step of managing a key for decrypting an encrypted E-mail, an authentication step of executing authentication of the use allowance of the managed key to said client based on authentication information sent from said client when said client requests to decrypt the encrypted E-mail, a decrypting step of decrypting ~~said~~ the encrypted E-mail using ~~said~~ the managed key in the server in the case where the use allowance is authenticated in said authentication step, and a transmission control step of controlling ~~said decrypted~~ to transmit the E-mail ~~so as to transmit~~ decrypted in said decrypting step to said client, ~~and wherein the program comprises a step of executing a use allowance step of executing the use allowance of a key for decrypting said encrypted E-mail to said server~~ the

PAGE 10/16 * RCVD AT 6/29/2005 7:10:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-38

client comprising a requesting step of requesting to decrypt the encrypted E-mail, an authentication information sending step of sending the authentication information for authentication in said authentication step, and a receiving step of receiving the decrypted E-mail ~~decrypted by said server~~ transmitted in said transmission step to the client.

PAGE 11/16 * RCVD AT 6/29/2005 7:10:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-38